LISTING OF CLAIMS:

1. (Currently Amended) A method of providing security in a gaming machine, the method comprising:

receiving a mechanical key in a **first** lock within said gaming machine**, said first lock being adapted to provide access to a first key accessible environment**;

reading a first source of indicia from said key, wherein said first source of indicia comprises information or data specific to said lock;

reading a second source of indicia, wherein said second source of indicia comprises biometric information specific to one or more users of said key;

analyzing said second source of indicia with respect to a stored biometric information file at a location separate from said key;

~~**authorizing a use of said key based on the readings of said first and second sources of indicia;**~~

~~**restricting access to said key accessible environment selectively based on one or more additional factors; and**~~

permitting access to said **first** key accessible environment **based on the readings of said first and second sources of indicia;**

receiving said mechanical key in a second lock about said gaming machine, said second lock being adapted to provide access to a second key accessible environment; and

denying or permitting access to said second key accessible environment based on the reading of said second source of indicia, wherein said first and second locks are different locks and said first and second key accessible environments comprise different regions with respect to said gaming machine.

2. (Original) The method of claim 1, wherein said first source of indicia comprises one or more physical characteristics of said key.

3. (Original) The method of claim 2, wherein said one or more physical characteristics of said key comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and at least a portion of an edge profile of said key.

4. (Original) The method of claim 1, further including the step of:

capturing live data reflective of one or more parameters associated with any other step.

5. (Canceled)

6. (Previously Presented) The method of claim 1, wherein said biometric information comprises fingerprint related information.

7. (Previously Presented) The method of claim 1, wherein said biometric information comprises at least one item selected from the group consisting of facial recognition, voice recognition, and retinal scan.

8. (Original) The method of claim 1, wherein said information specific to one or more users of said key is contained within one or more authorized user IDs.

9. (Original) The method of claim 8, further including the step of:

revoking a previously authorized user ID.

10. (Canceled)

11. (Currently Amended) A method of providing security in a **device having multiple** key accessible environment**s**, the method comprising:

receiving a key in a **first** lock**, said first lock being adapted to provide access to a first key accessible environment**;

reading a first source of indicia from said key, wherein said first source of indicia comprises information or data specific to said lock;

reading a second source of indicia, wherein said second source of indicia comprises biometric information specific to one or more users of said key;

analyzing said second source of indicia with respect to a stored biometric information file at a location separate from said key;

~~**authorizing a use of said key based on the readings of said first and second sources of indicia; and**~~

permitting access to said **first** key accessible environment **based on the readings of said first and second sources of indicia;**

receiving said mechanical key in a second lock, said second lock being adapted to provide access to a second key accessible environment; and

denying or permitting access to said second key accessible environment based on the reading of said second source of indicia, wherein said first and second locks are different

locks and said first and second key accessible environments comprise different regions about said device.

12. (Original) The method of claim 11, wherein said first source of indicia comprises one or more physical characteristics of said key.

13. (Original) The method of claim 12, wherein said one or more physical characteristics of said key comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and at least a portion of an edge profile of said key.

14. (Original) The method of claim 11, further including the step of:

capturing live data reflective of one or more parameters associated with any other step.

15. (Canceled)

16. (Previously Presented) The method of claim 11, wherein said biometric information comprises fingerprint related information.

17. (Previously Presented) The method of claim 11, wherein said biometric information comprises at least one item selected from the group consisting of facial recognition, voice recognition, and retinal scan.

18. (Original) The method of claim 11, wherein said information specific to one or more users of said key is contained within one or more authorized user IDs.

19. (Original) The method of claim 18, further including the step of:

revoking a previously authorized user ID.

20. (Original) The method of claim 11, wherein said information specific to one or more users of said key involves the use of an active PIN authentication.

21. (Original) The method of claim 11, further including the step of:

restricting access to said key accessible environment based on one or more additional factors.

22. (Original) The method of claim 21, wherein one additional factor includes the use of specified time periods.

23. (Original) The method of claim 11, wherein said key accessible environment comprises a gaming machine.

24. (Currently Amended) An apparatus, comprising:

a **first** key accessible environment;

a~~n~~ **first** electromechanical lock securing said **first** key accessible environment, wherein said **first** electromechanical lock is adapted to deny access to said **first** key accessible

environment unless a mechanical key having a correct first source of indicia is inserted into the lock and an authorization signal is provided based upon the verification of a correct second source of indicia with respect to the user of said mechanical key, wherein said second source of indicia comprises biometric information with respect to said user of said mechanical key;

a second key accessible environment;

a second electromechanical lock securing said second key accessible environment, wherein said second electromechanical lock is adapted to permit or deny access to said second key accessible environment based upon said second source of indicia with respect to the user of said mechanical key; and

an approval mechanism adapted to compare said biometric information with data stored separately from said mechanical key, wherein said approval mechanism is located separately from said mechanical key**, wherein said approval mechanism is adapted to permit access to each of said first and second key accessible environments based upon the identity of the user**.

25. (Original) The apparatus of claim 24, wherein said first source of indicia comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and at least a portion of an edge profile of said key.

26. (Canceled)

27. (Previously Presented) The apparatus of claim 24, wherein said biometric information comprises fingerprint related information.

28. (Original) The apparatus of claim 24, wherein second source of indicia involves the use of an active PIN authentication.

29-30. (Canceled)

31. (Currently Amended) A gaming machine adapted to accept a wager, play a game based on the wager, and grant an award based on the outcome of the game, comprising:

~~at least one~~ **a first** key accessible region containing one or more internal gaming machine components adapted for use in the acceptance of a wager, the play of a game, the granting of an award, or any combination thereof; ~~and~~

a~~n~~ **first** electromechanical lock securing said ~~at least one~~ **first** key accessible region, wherein said **first** electromechanical lock is adapted to deny access to said **first** key accessible region unless a mechanical key having a correct first source of indicia is inserted into the lock and an authorization signal is provided based upon the verification of a correct second source of indicia with respect to the user of said mechanical key, wherein said second source of indicia comprises biometric information with respect to said user of said mechanical key**;**

a second key accessible region containing one or more gaming machine components; and

a second electromechanical lock securing said second key accessible region, wherein said second electromechanical lock is adapted to permit or deny access to said second key accessible region based upon the identity of said user, as determined by said second source of indicia with respect to said user, and wherein said first and second electromechanical

locks are adapted to accept the same electromechanical key having a correct first source of indicia.

32. (Original) The gaming machine of claim 31, wherein said first source of indicia comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and at least a portion of an edge profile of said key.

33. (Canceled)

34. (Previously Presented) The gaming machine of claim 31, wherein said biometric information comprises fingerprint related information.

35. (Original) The gaming machine of claim 31, wherein second source of indicia involves the use of an active PIN authentication.

36. (Currently Amended) A method of providing security in a gaming machine, the method comprising:

receiving a key in a **first** lock **at or in said gaming machine**;

reading a user-based source of indicia **at said first lock**, wherein said user-based source of indicia comprises biometric information specific to one or more users of said key;

analyzing said ~~second~~ **user-based** source of indicia with respect to a stored biometric information file at a location separate from said key;

authorizing a use of said key **with respect to said first lock** based on an affirmative reading of said user-based source of indicia;

receiving said key in a second lock at or in said gaming machine;

reading said user-based source of indicia at said second lock;

analyzing said user-based source of indicia with respect to said stored biometric information file; and

authorizing or denying a use of said key with respect to said second lock based on the identity of said user as determined by the reading of said user-based source of indicia

~~**restricting access to said key accessible environment selectively based on one or more additional factors; and**~~

~~**permitting access to said gaming machine or a component thereof in the event that said key is a correct key for said lock**~~.

37. (Original) The method of claim 36, further including the step of:

capturing live data reflective of one or more parameters associated with any other step.

38. (Canceled)

39. (Previously Presented) The method of claim 36, wherein said biometric information comprises fingerprint related information.

40. (Previously Presented) The method of claim 36, wherein said biometric information comprises at least one type of information selected from the group consisting of fingerprint, facial recognition, voice recognition, and retinal scan information.

41. (Currently Amended) A universal key security system, comprising:

at least one computer server; and

one or more gaming machines in communication with said at least one computer server, wherein at least one of said one or more gaming machines comprises a~~n~~ **plurality of** electromechanical lock**s** securing ~~**at least one**~~ **a plurality of different** region**s** of said gaming machine,

wherein **each of** said **plurality of** electromechanical lock**s** is adapted to deny access to ~~**said at least one**~~ **its respective** region of said gaming machine unless a key having a correct first source of indicia is inserted into the lock and an authorization signal is provided based at least in part upon the verification of a correct second source of indicia with respect to the user of said mechanical key, wherein said second source of indicia comprises biometric information with respect to said user of said mechanical key**, wherein said system is adapted to provide access to different regions selectively based upon the identity of said user**.

42. (Canceled)

43. (Original) The universal key security system of claim 41, further including a database in communication with said at least one computer server.

44. (Original) The universal key security system of claim 43, wherein said database comprises at least one file containing information related to an authorized user of said universal key security system.

45. (Original) The universal key security system of claim 41, wherein said at least one computer server is adapted to capture live data associated with an attempt to access said at least one region of said gaming machine secured by said electromechanical lock.

46. (Original) The universal key security system of claim 41, wherein said authorization signal is provided at least in part through the use of said at least one computer server.

47. (Original) The universal key security system of claim 41, wherein said verification of a correct second source of indicia with respect to the user of said mechanical key is accomplished at least in part through use of said at least one computer server.